OWASP WTE:

An open environment for web application security.

Matt Tesauro
OWASP Foundation Board Member
OWASP Live CD / WTE
Project Lead
matt.tesauro@owasp.org

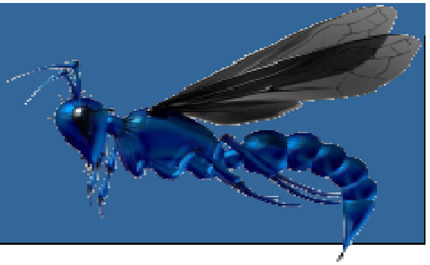
OWASP Software Assurance Day 2010

The OWASP Foundation
http://www.owasp.org

Presentation Overview

- Who am I and what's this OWASP Live CD thing anyway?
- Where are we now?
- Where are we going?
- How can I get involved?

About me



- Varied IT Background
  - Developer, DBA, Sys Admin, Pen Tester, Application Security, CISSP, CEH, RHCE, Linux+
- Long history with Linux & Open Source
  - First Linux install ~1998
  - DBA and Sys Admin was all open source
  - Contributor to many open source projects, leader of one

Project History and Goals

- Started as a Summer of Code 2008 project
- GOAL: Make application security tools and documentation easily available and easy to use
  - Compliment's OWASP goal to make application security visible
- Design goals
  - Easy for users to keep updated
  - Easy for project lead to keep updated
  - Easy to produce releases (more on this later)
  - Focused on just application security – not general pen testing

General goals going forward

- Showcase great OWASP projects
- Provide the best, freely distributable application security tools/documents in an easy to use package
- Ensure that the tools provided are easy to use as possible
- Continue to document how to use the tools and how the modules were created
- Align the tools with the OWASP Testing Guide v3 to provide maximum coverage

Where are we now?

- Current Release
  - OWASP WTE (about 2 weeks out, beta available)
- Previous Releases
  - AppSecEU May 2009
  - AustinTerrier Feb 2009
  - Portugal Release Dec 2008
  - SoC Release Sept 2008
- Overall downloads = 287,588 (of 2009-09-18)
  - ~4,396.4 GB of bandwidth since launch (Jul 2008)
  - Most downloads in 1 month = 81,607 (Mar 2009)

Available Tools: 26 'Significant'

OWASP Tools:

Web Scarab

a tool for performing all types of security testing on web apps and web services

Web Goat

an online training environment for hands-on learning about app sec

CAL9000

a collection of web app sec testing tools especially encoding/decoding

JBroFuzz

a web application fuzzer for requests being made over HTTP and/or HTTPS.

WSFuzzer

a fuzzer with HTTP based SOAP services as its main target

Wapiti

audits the security of web apps by performing "black-box" scans

DirBuster

a multi threaded Java app to brute force directory and file names

SQLiX

a SQL Injection scanner, able to crawl, detect SQL-i vectors

Available Tools: 26 'Significant'

Other Proxies:

- Burp Suite
- Paros
- Spike Proxy
- Rat Proxy

Scanners:

- w3af
- Grendel Scan
- Nikto
- namp
- Zenmap
- Fierce Domain Scanner

SQL-i:

- sqlmap
- SQL Brute

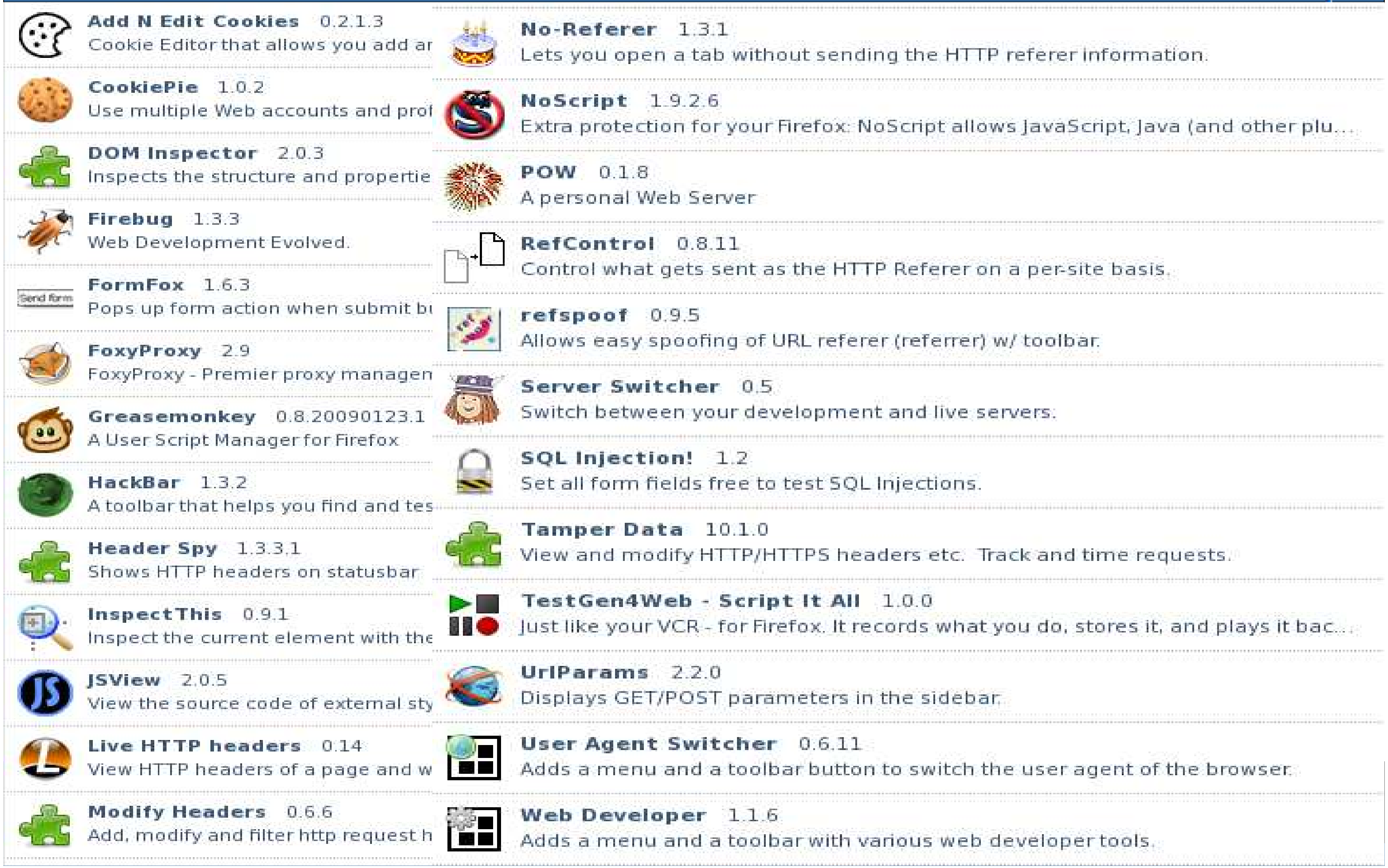
Duh:

- Firefox

Others:

- Metasploit
- Httprint
- Maltego CE
- netcat
- Wireshark
- tcpdump

Special features...



Add N Edit Cookies 0.2.1.3
Cookie Editor that allows you add ar

CookiePie 1.0.2
Use multiple Web accounts and prof

DOM Inspector 2.0.3
Inspects the structure and propertie

Firebug 1.3.3
Web Development Evolved.

FormFox 1.6.3
Pops up form action when submit bu

FoxyProxy 2.9
FoxyProxy - Premier proxy managen

Greasemonkey 0.8.20090123.1
A User Script Manager for Firefox

HackBar 1.3.2
A toolbar that helps you find and tes

Header Spy 1.3.3.1
Shows HTTP headers on statusbar

InspectThis 0.9.1
Inspect the current element with the

JSView 2.0.5
View the source code of external sty

Live HTTP headers 0.14
View HTTP headers of a page and w

Modify Headers 0.6.6
Add, modify and filter http request h

No-Referer 1.3.1
Lets you open a tab without sending the HTTP referer information.

NoScript 1.9.2.6
Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plu...

POW 0.1.8
A personal Web Server

RefControl 0.8.11
Control what gets sent as the HTTP Referer on a per-site basis.

refspoof 0.9.5
Allows easy spoofing of URL referer (referrer) w/ toolbar.

Server Switcher 0.5
Switch between your development and live servers.

SQL Injection! 1.2
Set all form fields free to test SQL Injections.

Tamper Data 10.1.0
View and modify HTTP/HTTPS headers etc. Track and time requests.

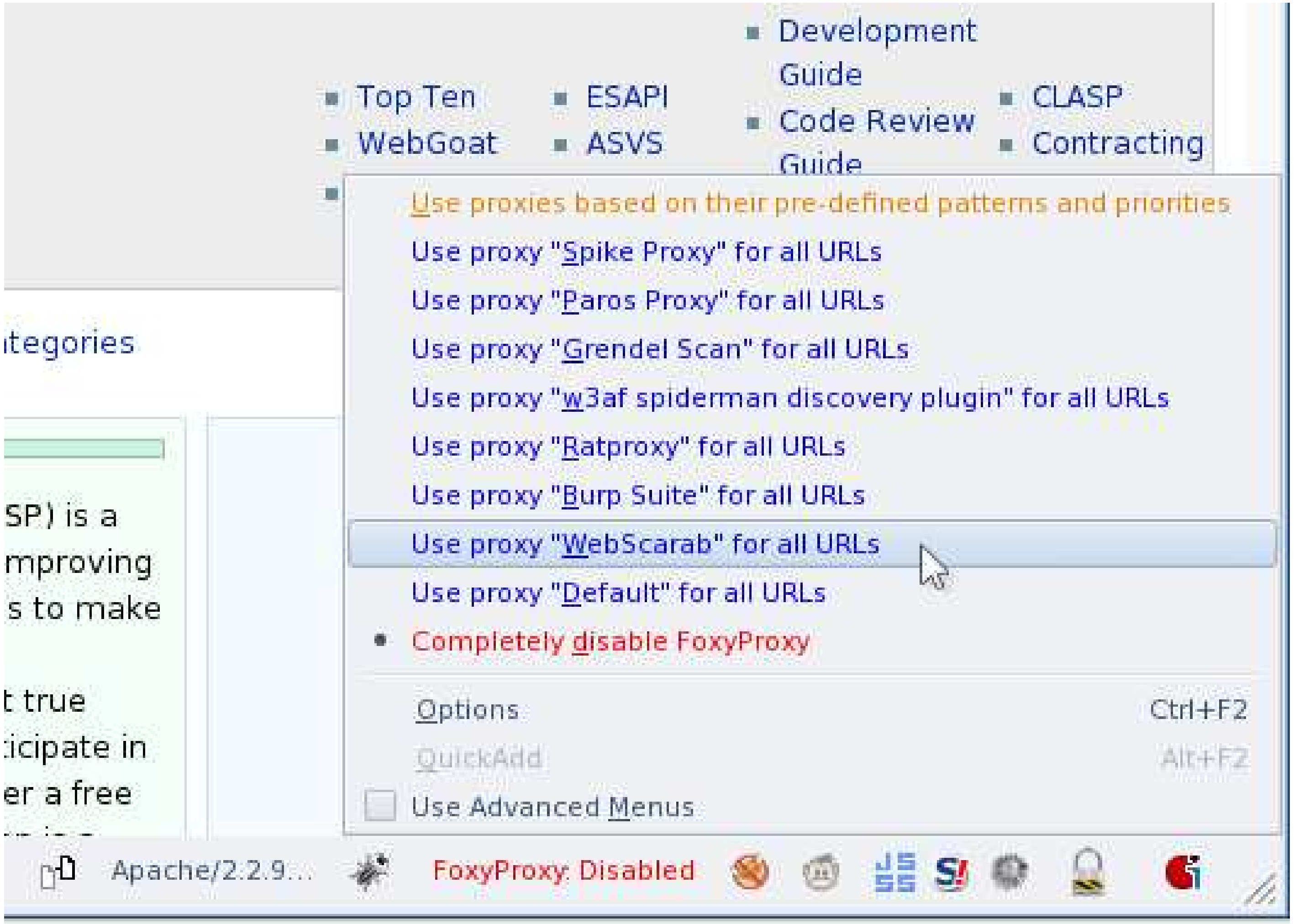
TestGen4Web - Script It All 1.0.0
Just like your VCR - for Firefox. It records what you do, stores it, and plays it bac...

UrlParams 2.2.0
Displays GET/POST parameters in the sidebar.

User Agent Switcher 0.6.11
Adds a menu and a toolbar button to switch the user agent of the browser.

Web Developer 1.1.6
Adds a menu and a toolbar with various web developer tools.

Special features...



- Top Ten
- WebGoat
- ESAPI
- ASVS
- Development Guide
- Code Review Guide
- CLASP
- Contracting

Use proxies based on their pre-defined patterns and priorities
Use proxy "Spike Proxy" for all URLs
Use proxy "Paros Proxy" for all URLs
Use proxy "Grendel Scan" for all URLs
Use proxy "w3af spiderman discovery plugin" for all URLs
Use proxy "Ratproxy" for all URLs
Use proxy "Burp Suite" for all URLs
Use proxy "WebScarab" for all URLs
Use proxy "Default" for all URLs
● Completely disable FoxyProxy

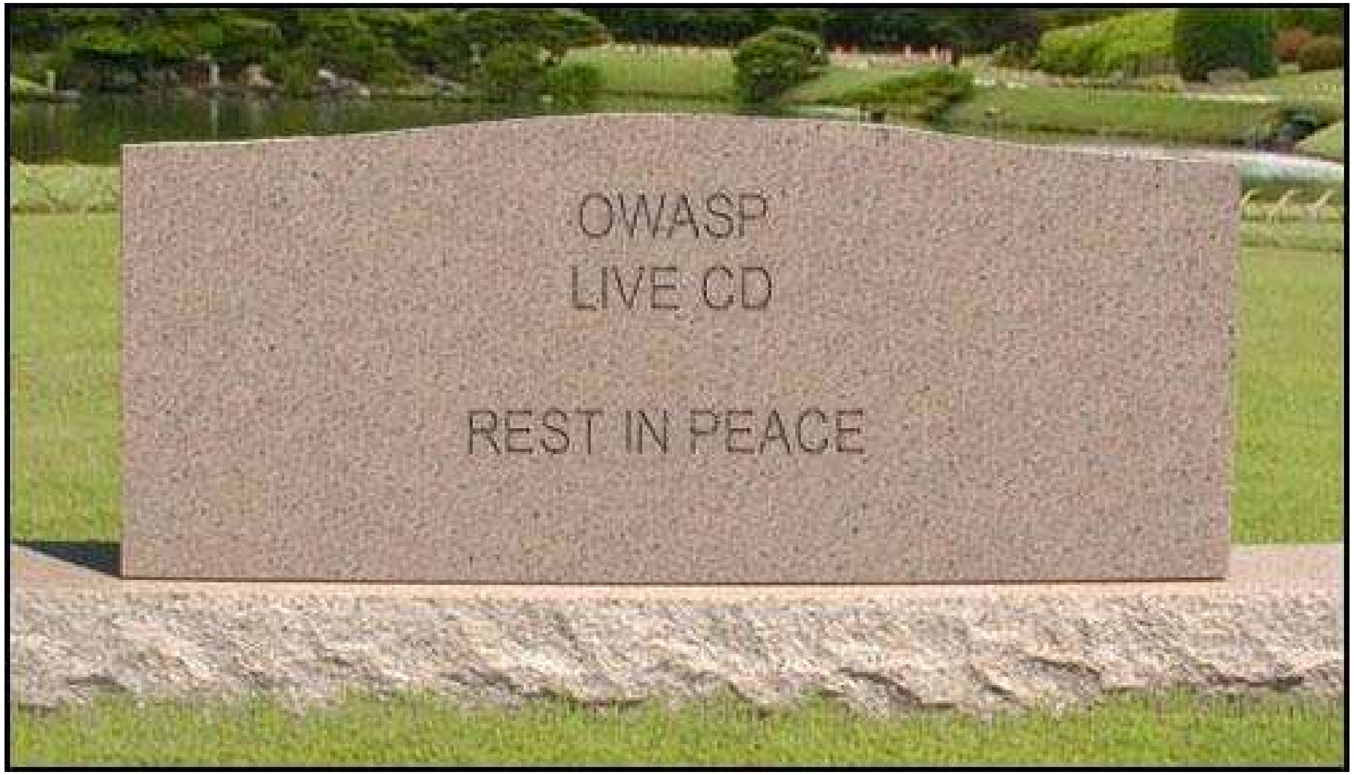
Options Ctrl+F2
QuickAdd Alt+F2
□ Use Advanced Menus

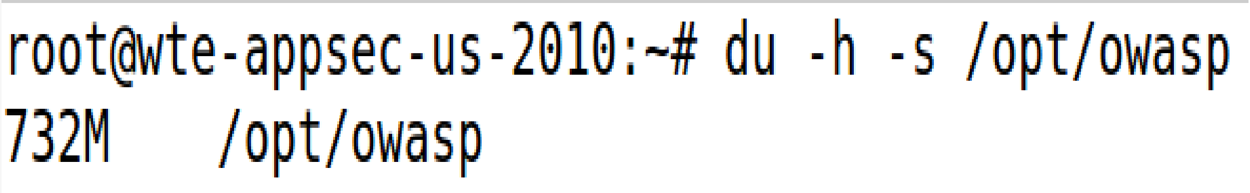
Documentation available

- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP and OpenSamm
  - Top 10 for 2010
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books
    - CLASP, Top 10 2010, Top 10 + Testing + Legal, WebGoat and Web Scarab, Guide 2.0, Code Review

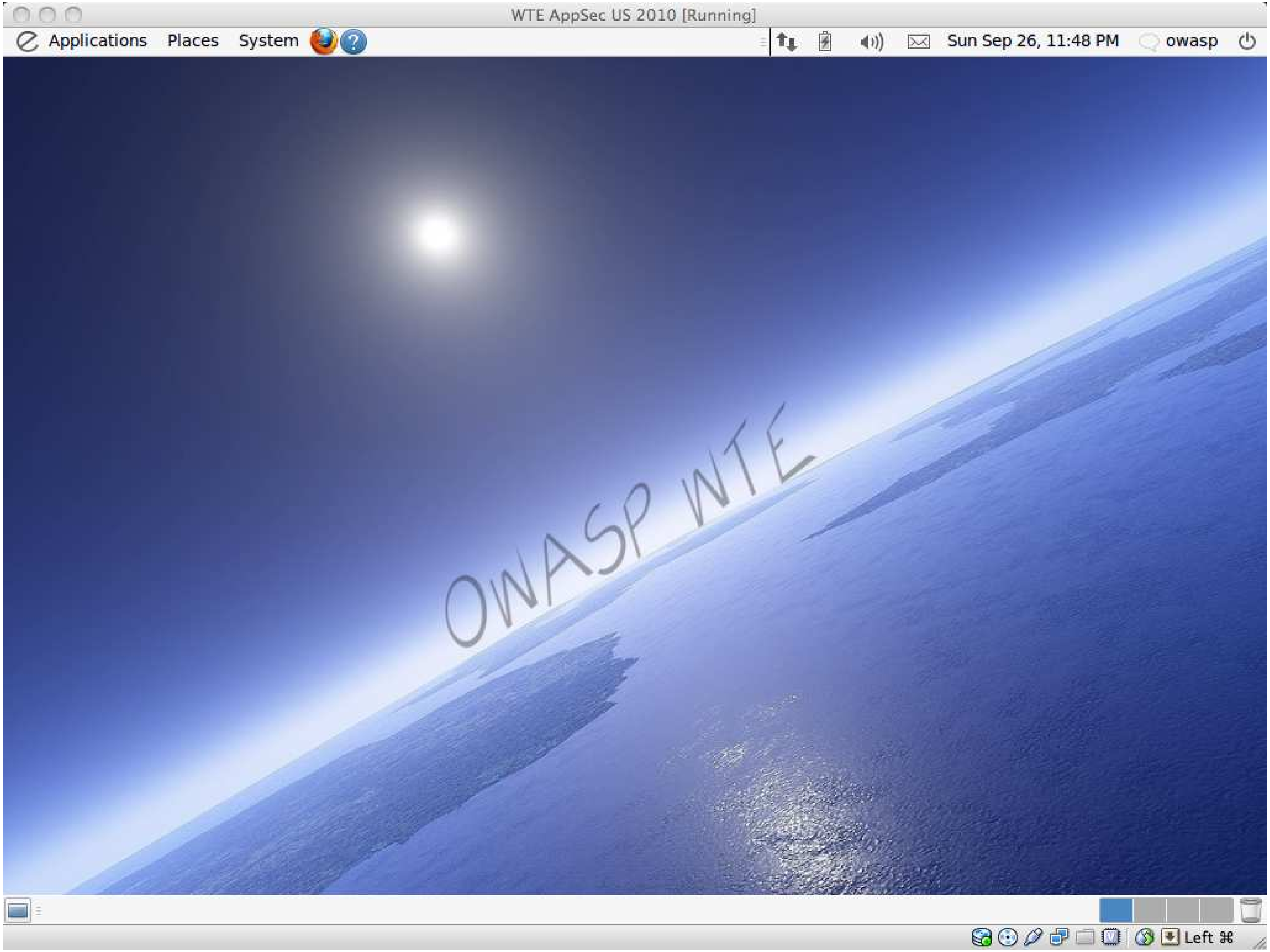
- Others
  - WASC Threat Classification, OSTTMM 3.0 & 2.2

News Flash!

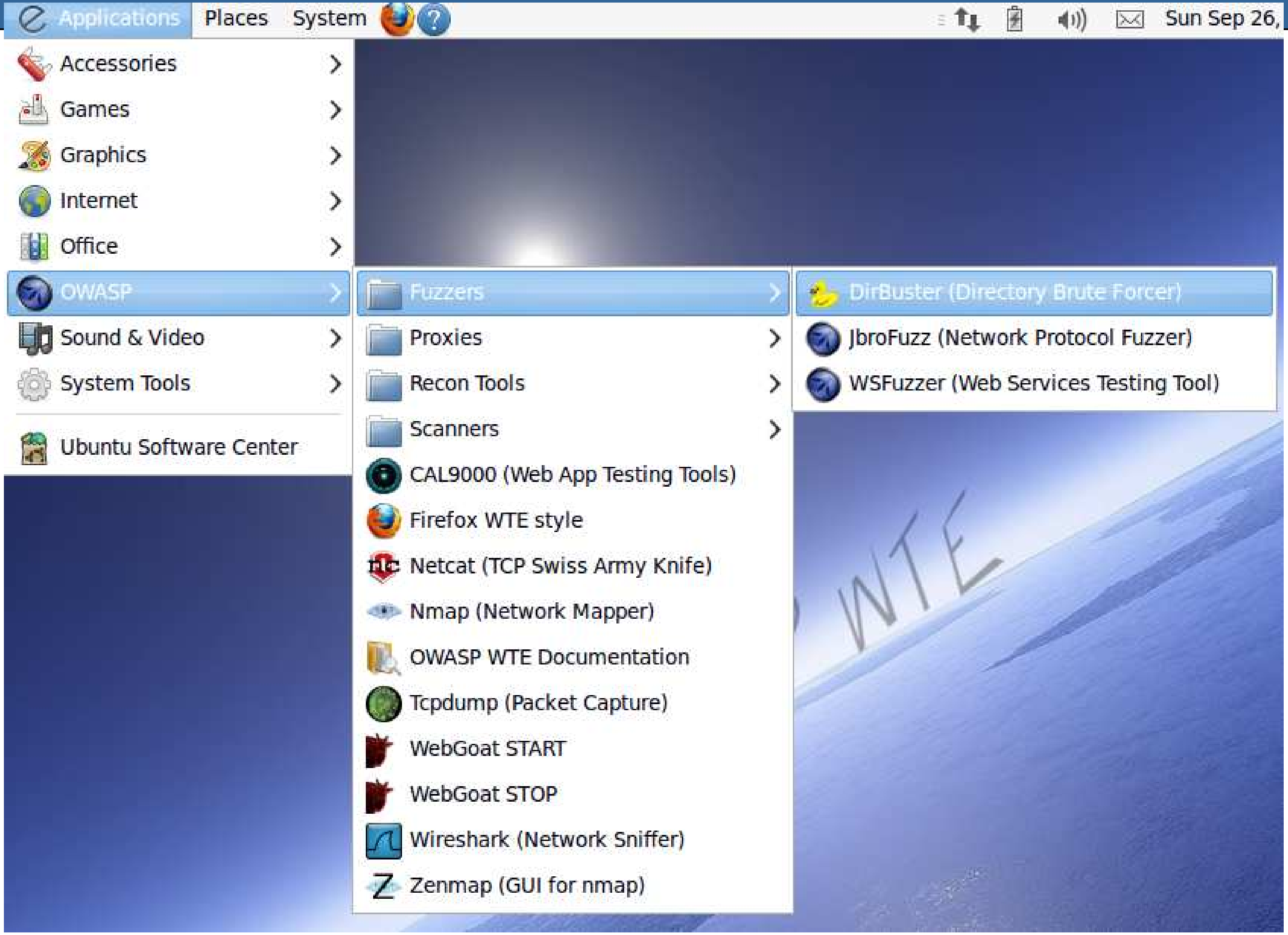




```
root@wte-appsec-us-2010:~# du -h -s /opt/owasp
732M    /opt/owasp
```

WTE AppSec US 2010 [Running]
Applications
Places
System
Sun Sep 26, 11:48 PM
owasp
OWASP WTE
Left ⌘

The OWASP menu



Where are we going?

- The cool fun stuff ahead
  - Virtual Installs & others
  - Builder vs Breaker
  - Ubuntu based
  - OWASP Education Project
  - Minor release tweaks
  - Crazy Pie in the Sky idea
  - WTE Cloud Edition

Project Tindy & Aqua Dog

- Project Tindy
  - OWASP Live CD installed to a virtual hard drive
  - Persistence!
  - VMware, Virtual Box & Paralles

- Project Aqua Dog
  - OWASP Live CD on a USB drive
  - VM install + VM engine + USB drive = mobile app sec platform
- Wubi – non-destructive dual boot

Builder vs Breaker

Builder is where the ROI is

But darn it,
breaking is really fun.

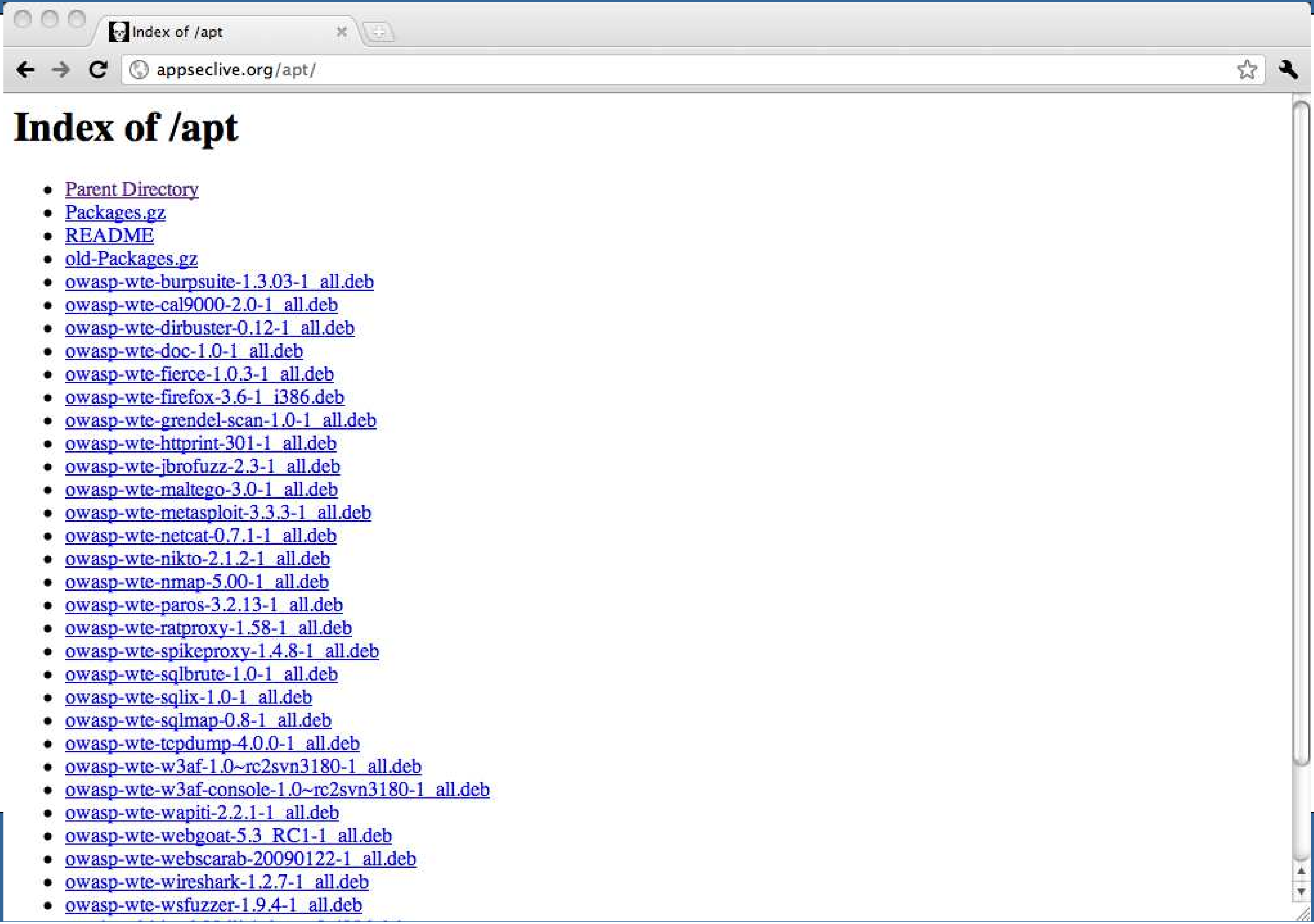
Builder tools coming in future releases.

(Thanks Top Gear!)

Live CD now Ubuntu based

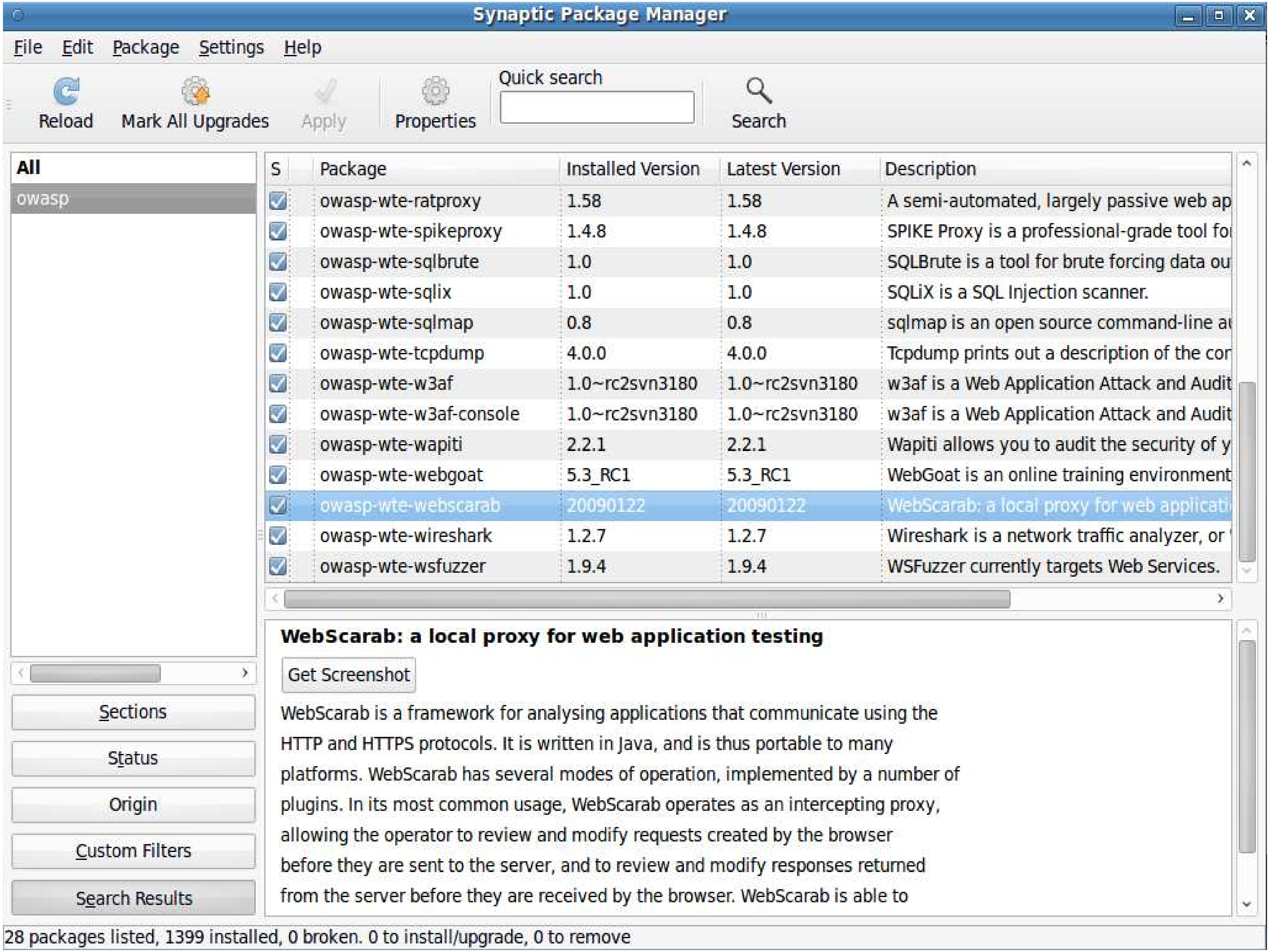
- Create .deb packages for every tool
- Create a repository for packages
- Add dependency info to packages
- Brings the 26,000+ existing packages to the Live CD
- Currently tied to Ubuntu 10.04 LTS

The repository (beta)



Index of /apt

- Parent Directory
- Packages.gz
- README
- old-Packages.gz
- owasp-wte-burpsuite-1.3.03-1_all.deb
- owasp-wte-cal9000-2.0-1_all.deb
- owasp-wte-dirbuster-0.12-1_all.deb
- owasp-wte-doc-1.0-1_all.deb
- owasp-wte-fierce-1.0.3-1_all.deb
- owasp-wte-firefox-3.6-1_i386.deb
- owasp-wte-grendel-scan-1.0-1_all.deb
- owasp-wte-httprint-301-1_all.deb
- owasp-wte-jbrofuzz-2.3-1_all.deb
- owasp-wte-maltego-3.0-1_all.deb
- owasp-wte-metasploit-3.3.3-1_all.deb
- owasp-wte-netcat-0.7.1-1_all.deb
- owasp-wte-nikto-2.1.2-1_all.deb
- owasp-wte-nmap-5.00-1_all.deb
- owasp-wte-paros-3.2.13-1_all.deb
- owasp-wte-ratproxy-1.58-1_all.deb
- owasp-wte-spikeproxy-1.4.8-1_all.deb
- owasp-wte-sqlbrute-1.0-1_all.deb
- owasp-wte-sqlix-1.0-1_all.deb
- owasp-wte-sqlmap-0.8-1_all.deb
- owasp-wte-tcpdump-4.0.0-1_all.deb
- owasp-wte-w3af-1.0~rc2svn3180-1_all.deb
- owasp-wte-w3af-console-1.0~rc2svn3180-1_all.deb
- owasp-wte-wapiti-2.2.1-1_all.deb
- owasp-wte-webgoat-5.3_RC1-1_all.deb
- owasp-wte-webscarab-20090122-1_all.deb
- owasp-wte-wireshark-1.2.7-1_all.deb
- owasp-wte-wsfuzzer-1.9.4-1_all.deb



S	Package	Installed Version	Latest Version	Description
☑	owasp-wte-ratproxy	1.58	1.58	A semi-automated, largely passive web ap
☑	owasp-wte-spikeproxy	1.4.8	1.4.8	SPIKE Proxy is a professional-grade tool fo
☑	owasp-wte-sqlbrute	1.0	1.0	SQLBrute is a tool for brute forcing data ou
☑	owasp-wte-sqlix	1.0	1.0	SQLiX is a SQL Injection scanner.
☑	owasp-wte-sqlmap	0.8	0.8	sqlmap is an open source command-line a
☑	owasp-wte-tcpdump	4.0.0	4.0.0	Tcpdump prints out a description of the cor
☑	owasp-wte-w3af	1.0~rc2svn3180	1.0~rc2svn3180	w3af is a Web Application Attack and Audit
☑	owasp-wte-w3af-console	1.0~rc2svn3180	1.0~rc2svn3180	w3af is a Web Application Attack and Audit
☑	owasp-wte-wapiti	2.2.1	2.2.1	Wapiti allows you to audit the security of y
☑	owasp-wte-webgoat	5.3_RC1	5.3_RC1	WebGoat is an online training environment
☑	owasp-wte-webscarab	20090122	20090122	WebScarab: a local proxy for web applicati
☑	owasp-wte-wireshark	1.2.7	1.2.7	Wireshark is a network traffic analyzer, or
☑	owasp-wte-wsfuzzer	1.9.4	1.9.4	WSFuzzer currently targets Web Services.

WebScarab: a local proxy for web application testing

WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. It is written in Java, and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plugins. In its most common usage, WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser. WebScarab is able to

28 packages listed, 1399 installed, 0 broken. 0 to install/upgrade, 0 to remove

OWASP Education Project

- Natural ties between these projects
  - Already being used for training classes
  - Need to coordinate efforts to make sure critical pieces aren't missing from the OWASP WTE
  - Training environment could be customized for a particular class thanks to the individual modules
    - Student gets to take the environment home
  - As more modules come online, even more potential for cross pollination
  - Builder tools/docs only expand its reach
  - Kiosk mode?

Crazy Pie in the Sky idea

- .deb package + auto update + categories = CD profiles
  - Allows someone to customize the OWASP WTE to their needs
  - Example profiles
    - Whitebox testing
    - Blackbox testing
    - Static Analysis
    - Target specific (Java, .Net, ...)
  - Profile + VM
    = custom persistent work environment

How can you get involved?

- Join the mail list
  - Announcements are there – low traffic
- Post on the AppSecLive.org forums
- Download an ISO or VM
  - Complain or praise, suggest improvements
  - Submit a bug to the Google Code site
- Create deb package of a tool
  - How I create the debs will be documented, command by command and I'll answer questions gladly
- Suggest missing docs or links
- Do a screencast of one of the tools being used on the OWASP WTE

Learn More

- OWASP Site:

  http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

  or just look on the OWASP project page (release quality)
  http://www.owasp.org/index.php/Category:OWASP_Project

  or Google "OWASP Live CD"

- Download & Community Site:
  http://AppSecLive.org

- Previously: http://mtesauro.com/livecd/

Questions?

Its Demo time!

DEMO AHEAD

Watch out for explosion
and demo gremlins